Diyala Journal of Engineering Sciences

Journal homepage: https://djes.info/index.php/djes

ISSN: 1999-8716 (Print); 2616-6909 (Online)

Modeling and Detection of Cyber and Physical Attacks on the Control Unit of PV Farm System

Aqeel Sajjad Shaeel[1,*], Huda Hussein Abed[2], Ahmed Fahim Al-Baghdadi[3]

[1]Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq.
[2]Department of Communication Techniques, Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq.
[3]Department of Medical Devices Techniques, Najaf Technical Institute, Al-Furat Al-Awsat Technical University, Najaf, Iraq.

ARTICLE INFO

Article history:
Received September 5, 2024
Revised May 6, 2025
Accepted May 11, 2025
Available online June 1, 2025

Keywords:
TDA
SCF
PV Farm
MPPT
Cybersecurity

ABSTRACT

The use of solar panels is becoming increasingly important now as a source of renewable energy. With the different systems designed to invest solar energy and the different electronic attacks on renewable energy systems, the importance of designing a photovoltaic system with different features appears in terms of detecting the attack on the input of the control unit to the system, and thus knowing the electronic attacks targeting the control unit. In this paper, a solar farm system based on cyberattack detection is designed and analyzed using MATLAB Simulink. First, the proposed system detects and identifies cyberattacks, such as Time Delay Attacks (TDA), on the PV controller. Second, it diagnoses physical attacks, including Short Circuit Faults (SCF), and evaluates their impact on the photovoltaic controller. The simulation comprises TDA and SCF attacks and their impact on current and voltage waveforms in the PV system. These types of attacks mainly depend on delaying or changing the triggering signal, which leads to an effect on the output signals. In addition, the modulation-index feature is adopted in verifying the presence of attacks and diagnosing their type on the photovoltaic farm configuration, it reaches its highest value of 0.91 when the solar farm is operating properly. On the other hand, it is disturbed and fluctuates to reach 0.66 and 0.16 in the case of SCA and TDA, respectively. The Simulink results demonstrate that the electronic attack affected the current and voltage for each solar cell at the attack simulation time of 0.4 seconds.

1. Introduction

The energy sector has undergone quick technological advancement and integration, leading to important changes in electricity generation, distribution, and usage [1].

The network of electricity that achieves the bidirectional flow of electricity and information through utilizing digital techniques for communication, is known as a smart grid. The objective of the smart grid is to convert networks of traditional electricity into the contemporary grid with the aid of information and dispatch technologies [2]. The growing request for clean and renewable energy led to the evolution of solar photovoltaic (PV) systems. It represented an alternative to conventional power generation strategies according to its ability to generate electricity straight from the sunlight, and also when attached to the smart grid, can provide electricity to the entire grid [3-4].

The benefits of integrating the smart grid with photovoltaic panels have become increasingly apparent in recent years. Those integration systems are becoming diffuse greatly due to their feature in increasing the

* Corresponding author.
E-mail address: aqeel.sajjad@atu.edu.iq
DOI: 10.24237/djes.2025.18210

This work is licensed under a Creative Commons Attribution 4.0 International License.

employment of renewable energy sources and supplying energy efficiency [5]. However, the performance of solar PV systems depends on the capability to exercise the maximum power of the solar panels, which are influenced by diverse factors such as irradiance, temperature, and shading [3,6]. Generally, the temperature and the variations in solar irradiation are considered the most impacting factors for PV generation systems [7]. According to the mitigation in the cost of materials that make PV panels and also solar energy sustainability, the utilization of PV networks has been growing recently around the globe [8]. PV panels are composed of semiconductor materials [9]. When the light from the sun falls on the PV panel surface, the energy from the photons is absorbed by the semiconductor materials. This procedure is called the photoelectric effect. That procedure relieves electrons from their atomic constraint, thus resulting in an electric current. The produced electric current is in the state of direct current (DC) [10]. The generated direct current is then transformed into alternating current (A.C.), usually utilizing inverters and additional components [11], to make this electricity applicable to most domestic equipment and the electrical grid [10].

The major disadvantage of generating electrical power from solar energy is that the generated power is not constant over the day due to the continual changes in atmospheric conditions. Further, the efficiency of converting solar energy into electrical energy is very low. Thus, maximum power point tracking that is abbreviated as MPPT represents the fundamental part of the smart grid-tied solar PV systems [12] to guarantee optimal energy creation from PV systems, particularly under altering circumferential conditions [13]. MPPT algorithms confirm that the panels work at their maximum power, which is important to achieve overall efficiency of power production procedures [14-15]. Sometimes, Solar PV systems can generate more electricity than is required or consumed, essentially through high summer heat. This excess energy is kept in the batteries [16]. Figure 1 shows a typical form of PV solar energy system [17]. PV panels are being advanced for commercialized employment such as rooftop PV installations and PV farms [18].

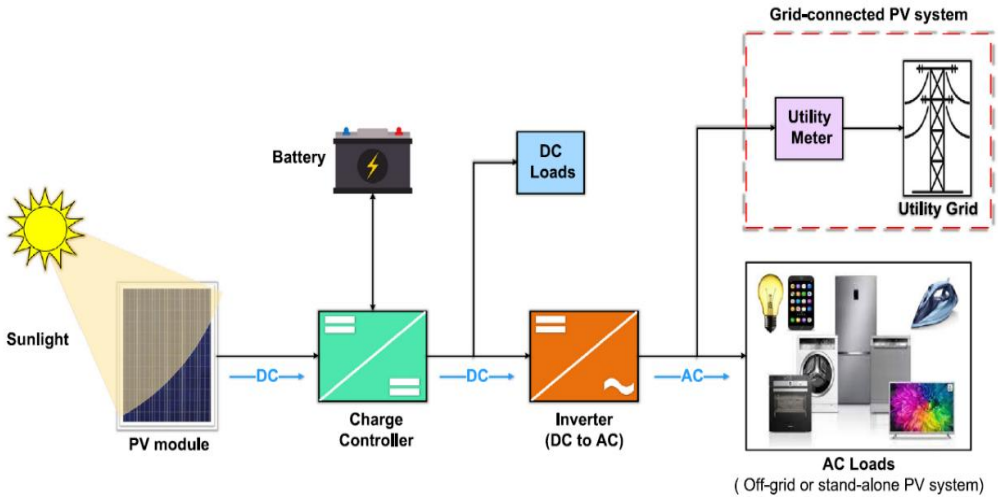


Figure 1. Typical form of PV solar energy system [15]

With the rapid growth and increasing importance of solar energy, and its connection with smart grids, vulnerabilities, and cyberattacks have also greatly grown [19]. Thus, protecting photovoltaic (PV) systems against cyberattacks and guaranteeing their safety is considered important to ensure the reliability of the electric power grid. Existing studies on the cybersecurity of the smart grid predominantly concentrate on cyber-attacks that influence the reliability and availability of the grid instead of the behavior of power electronics substations. This tendency is due to the rising permeation of utilizations via the Internet of Things (IoT). PV

systems are innately discontinuous, and that leads to specific challenges in determining the normal behavior, the Opposite of settlement behavior. Thus, the algorithms of cybersecurity must be more accurately created and customized for the detection of attacks. Cybersecurity of PV systems is considered an ingredient of smart grid security which participates in overall grid security [20]. Time Delay Attack (TDA) and Short Circuit Fault (SCF) respectively, are considered one of the dangerous techniques used by attackers for malicious purposes, and we will adopt them in this study and demonstrate their impact.

It is essential to have a comprehensive knowledge of the potential cybersecurity vulnerabilities concerning this complex infrastructure of the connectivity of smart grids with solar PV systems. Numerous studies have handled cybersecurity in smart grids integrating PV systems [1]. Effective and quick detection of potential attacks is critical to ensure the PV system's normal operation and maximum output power.

Qi Li, et al. [21] have applied data-driven methods to data from Micro-Phasor Measurement Units (μPMU) for detect the cyberattacks, where μPMUs are most popular for implementing intrusion detection. Their proposed convolutional neural network (CNN) model achieved the desired performance with the best accuracy reaching 99.23% and the best F1 score of 0.9963.

Fangyu Li, et al. [22] proposed a series of deep learning-based diagnostic solutions for information integrity attacks on smart grids of PV systems, whether in DC/DC or DC/AC inverter. In their work, they relied on (MLSTM) multi-layer long short-term memory grids to utilize time-series signal data due to current and voltage metrics and sensors in PV farms.

Xue Gao et al. [23] developed a comprehensive framework for assessing and diagnosing threats to cyber-physical security in distribution networks. The framework comprises three prominent sections. Firstly, cyber-physical system modeling. Secondly, threat identification with cyberattack models, and lastly, impact quantification.

JINAN ZHANG et al. [24] presented a technique via machine learning to detect cyber-attacks on (PV) farms employing point of common coupling (PCC) sensors only. Firstly, A comprehensive PV farm cyberattack model was developed to consider the variation in operating conditions. After that, a convolution neural network (CNN) that uses μPMU in addition to figures of merit was suggested and made comparison with other techniques. It is shown from their results that the proposed model can achieve sufficient detection accuracy and robustness under different attack scenarios.

THUNCHANOK KAEWNUKULTORN et al. [25] evaluated an intrusion detection procedure for smart grid apparatuses. Their findings depict that inverters from various manufacturers have diverse vulnerability scales to cyber-attacks. Most of the replies to the cyberattacks can be seized by calculating the power gush locally and externally via the grid manipulator and then comparing the factual power gush to the expected grid power gush.

Lulu Guo et al. [26] used time-frequency domain features to present the cyberattack detection for PV Farms. When comparing their proposed method to the current detection methods that use only micro phasor measurement units (μPMU) as input to the deep network, the test accuracy was modified (from 50%-60% to 98%).

In this paper, a solar farm system based the cyberattack detection is designed and analyzed using MATLAB Simulink. Firstly, detect and identify cyber-attacks caused by Time Delay Attack (TDA) on the PV grid based on its controller. Secondly, detect and identify physical attacks due to SCF and the impact on waveforms introduced into the control unit. After that, the effects of the attacks are simulated to observe their impact on the waveforms and diagnose the presence of the attacks on the PV solar farm configuration. The contributions of this study are summarized as:

1. A framework is developed that effectively detects and identifies the cyber and physical attacks at the controller of the solar farms.

2. The effects of TDA and SCF on controllers based on waveforms are analyzed and presented.
3. A completely new metric is developed and implemented in both attack detection and diagnosis, resulting in sensitive attack awareness as well as accurate analysis of attack type and severity.

The outline paper is as follows: Section 2 depicts the PV farm with Cyberattacks. In section 3, specifics of the suggested PV Farm model are presented. Simulink results are described in Section 4. Finally, the section demonstrates the conclusion of the paper.

2. PV Farm with Cyberattacks

Transferring sensitive information in total secrecy via the communication media has become essential [27]. Therefore, the existence of cybersecurity is necessary to rescue the digital environment [28].

Cybercriminals can utilize the smart grid telecommunication to venture large-scale aggression, such as Denial of Service (DoS): which Disrupts communication by overwhelming the network with traffic. Time Delay Attacks (TDA): Introduce malicious delays into communication systems, disrupting the operation of the control unit, False Data Injection Attacks (FDIA): manipulate sensor data to mislead the control system, Replay attacks abbreviated as (RA): Delay sensors data via repeat the same control signal, time synchronization attacks abbreviated as (TSA): It targets timing information and vulnerabilities in detecting false data to manipulate the measurements of meters, Load Redistribution Attacks abbreviated as (LRA): It targets economic Dispatch (ED) by retransmitting the resulting output. Thus, the fake ED can force the station into an uneconomical operating state, and other attack techniques. The developments of the aforementioned cyberattacks can be dangerous, and lead to significant losses, extending among economic losses to blackout losses and disruption to vital infrastructure. Also, they can lead to the stealing of sensitive information, such as company and customer data [29].

Thus, the great development that has occurred in solar energy farms can be very dangerous in the event of attacks. Since the systems depend on and require high accuracy in the control system, hence any error, especially if it is for sabotage, can be disastrous. Therefore, this research is important to address these problems. As a result, the simulation of this study models both TDA and SCF attacks and their impact on current and voltage waveforms in the PV system. These types of attacks mainly depend on delaying or changing the triggering signal times, which leads to a segregant effect on the output signals.

Figure 2 shows the diagram of the solar farm with cyberattacks. The solar panels are connected physically to the grid via the DC/DC converters, DC/AC inverters, and then grid-linked transformers. Then the primary components and control unit are attached via a cyber grid. The red color is attributed to possible cyberattacks on the control center (for example, data integrity attacks (DIA) on control signals, inverter feedback, and some unusual delay that is injected into the control signal). These attacks will damage the grid performance and the electronic converters. On the other hand, physical attacks can threaten the grid instruments (for example, short circuit faults SCF, capacitor bank cut-off, and abnormal load) [30]. Delays in the flow of information in a smart grid can significantly affect the performance of controllers. Signal transmissions over power line communications or wireless communication networks can cause these delays. Cyber-attacks such as TDA attacks introduce time delays. Time delays can also be introduced into the system through time synchronization of signals measured by GPS and analog-to-digital (A/D) conversions by signal measurement units such as remote terminal units (RTUs) and phasor measurement units (PMUs) [31–33]. Communication delays can also be associated with the opening and closing of circuit breakers on transmission and distribution lines after a fault occurs in smart grid systems. Obtaining the control signal at the right moment is essential for system control. TDA affects the system by randomly delaying the transmission and reception of packets, thus

pushing the control center out of its normal values and losing the synchronization built into the control signals, which can lead to faults or damage to the power system.

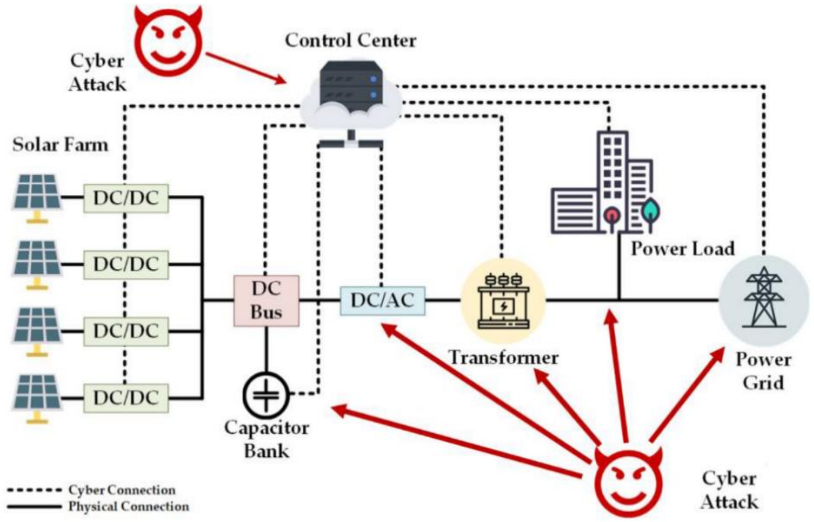
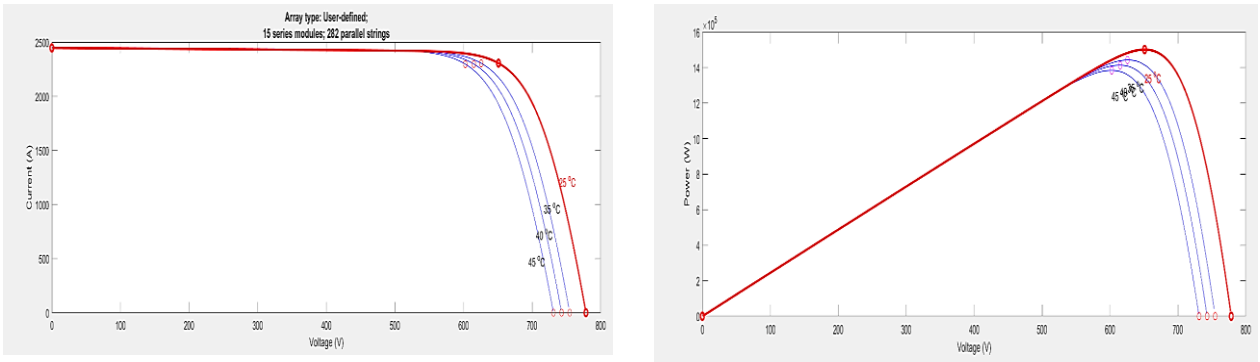


Figure 2. Cyberattacks on the solar farm [28]

3. Proposed PV farm model

A PV farm with 2 PV arrays is designed using MATLAB Simulink. Each PV array consists of strings of PV modules connected in parallel, with the modules in each string connected in series. Figure 3 shows the I-V and P-V characteristics of the proposed PV farm at different temperatures.

Figure 4 illustrates a fundamental diagram of the proposed system. This diagram serves as a visual representation of the essential components and their interconnections within the system.



a) b)

Figure 3. I and P with respect to V at different temperatures, a) I-V characteristics, b) P-V characteristics

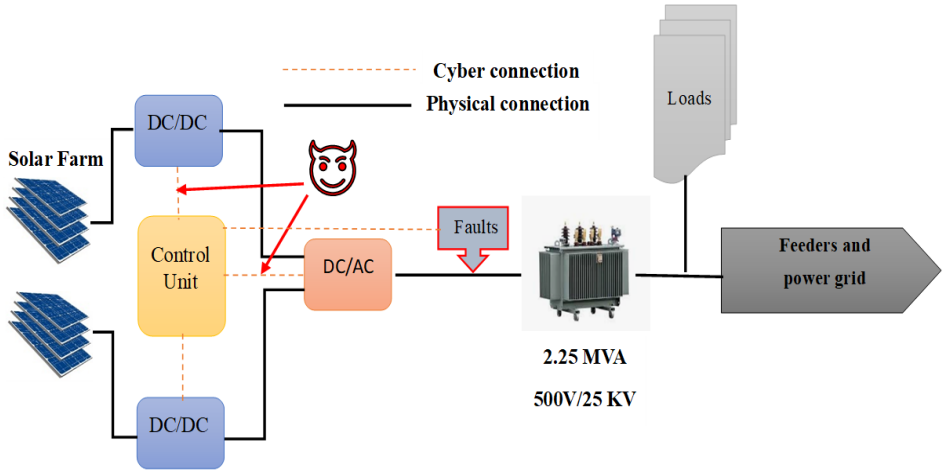


Figure 4. PV farm of our work consists of the attacks

The two PV arrays are connected for the two boost converters, respectively. Maximum Power Point Trackers algorithm (MPPT) is utilized for providing the control mechanism for each boost converter according to the Perturb and Observe manner. After that, the boost converter outputs are linked to the converter through the common DC bus. A DC voltage regulator is required for the controller processes of the converter, then a 3-phase coupling transformer is utilized for the connection of the selected converter to the required grid network.

To delve deeper into the functionality and potential applications, let us examine the various parts that can be utilized to simulate an electronic attack. The diagram in Figure 5 provides a detailed presentation of the control center within a solar cell system.

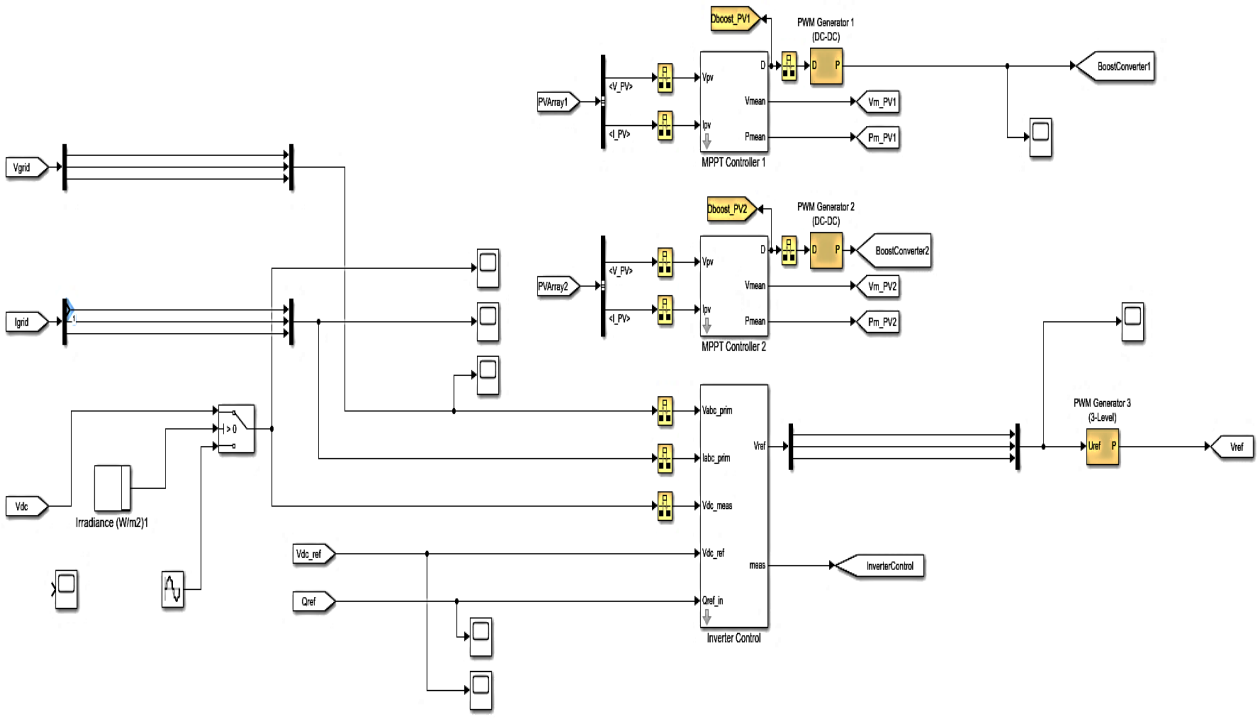


Figure 5. The detailed representation of the control system involves attack modeling within the solar cell system

This control system plays a pivotal role in ensuring the efficient performance of the solar cells by generating the necessary control signals that the inverter utilizes to produce the final output signal. The importance of this control system cannot be overstated, as it is considered a major component that regulates the performance and functions of the entire solar energy system. The attack system has also been added, which is based on the TDA strategy in our research. Which in turn affects the sensor measurements at a certain period of time and replaces them with another period of time during the time scenario, thus leading to a delay in receiving or sending packets and control signals, which leads to damage to vital devices and energy grid transactions.

To detect the temporal delay of a cyberattack early, an algorithm shown in Figure 6 was designed that adopts one of the important metrics to obtain a figure of merit from waveform data. To evaluate the total harmonic distortion through the extracted PCC waveform distortions, THD (total harmonic distortion) can be used in regarding as a Figure of merit. By taking advantage of THD values, the accuracy of PCC waveforms can be evaluated by system operators quickly in real-time [24]. Where the current THD waveform of the PCC is estimated by a dual-spectral interpolated line FFT and is represented according to eq.1[34], [35].

$$THD_I = \frac{\sqrt{\sum_n^H I_n^2}}{I_{fund}} \quad (1)$$

Where: H is the harmonic order; In is the value of the harmonic current n; I_{fund} is the fundamental current size.

A traditional method was adopted to calculate THD, according to Equation 1. The proposed method relies on analyzing the harmonics resulting from the Fast Fourier Transform (FFT) of the electrical signal. The fundamental frequency and higher harmonics are extracted, and sudden changes in the levels of these harmonics are then compared with pre-determined threshold values using the equation. Any excess of the normal threshold is an indication of an attack or abnormal operating condition.

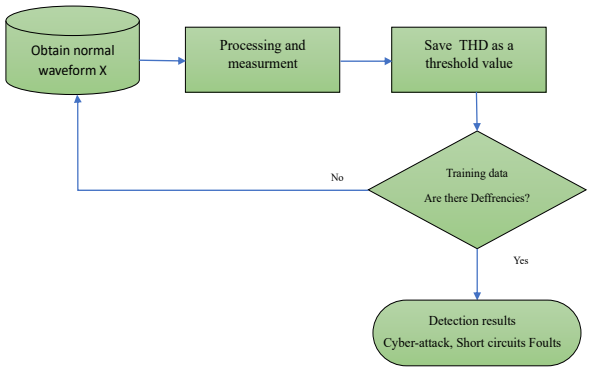


Figure 6. The proposed detection algorithm.

Although the algorithm is efficient at detecting attacks in real time, it lacks a precise identification of the type of attack. Therefore, we employed the Mod-Index metric alongside THD by monitoring it in real time. It can be monitored by a sudden drop or increase in the Mod-index without a change in solar irradiance or load, or disturbances in the modulation frequency (PWM) or duty cycle. However, the method of generating it is affected by the MPPT algorithm and is defined by Eq. 2:

$$m_a = \frac{V_{ref.}}{V_{carrier}} \quad (2)$$

Where: m_a The Mod-index is usually close to 0.9, which is considered ideal for the nature of the signal. $V_{ref.}$: Reference voltage generated by the MPPT algorithm (usually a sine wave if using SPWM) and $V_{carrier}$: Carrier voltage is usually a signal with constant frequency and amplitude.

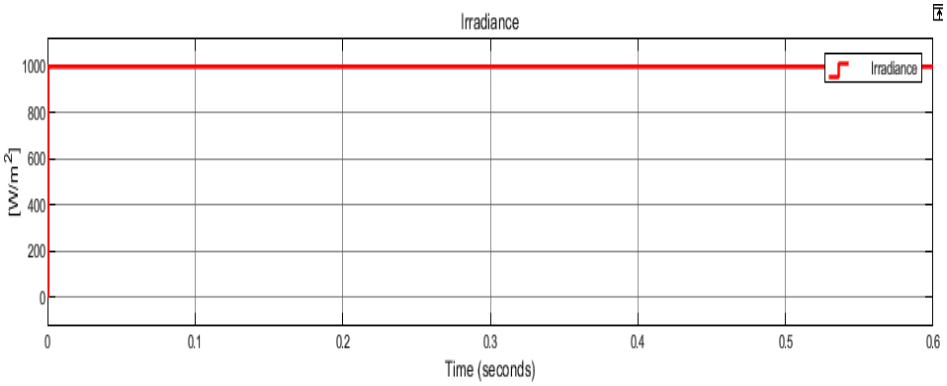
The MPPT algorithm calculates the optimal operating point (voltage or current) and assigns it to the inverter. This threshold value is used to generate the reference signal that is compared to the carrier wave. Therefore, a change in the MPPT output leads to a change in the Mod-index.

This method provides a fast and efficient response, without the need for complex tools such as the wavelet transform, which is more complex to implement and analyze than the FFT [36]. The traditional RMSE method also relies on monitoring the effective value, but it is unable to distinguish between the quality of harmonics or subtle changes in the frequency spectrum [18].

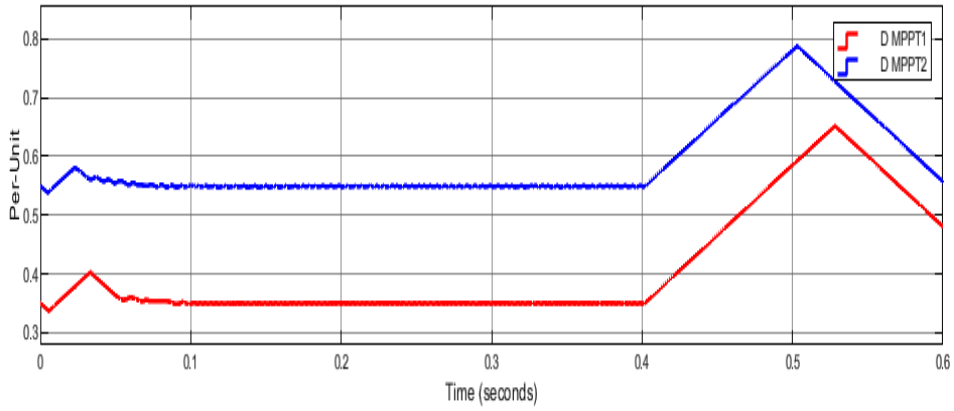
4. Simulink results

The control system of the proposed method, that was demonstrated in Figure 5 primary responsibility for monitoring and regulating various parameters to optimize the conversion of solar energy into electrical power. By generating precise control signals, it ensures that the inverter can accurately convert (DC) produced by the solar cells into (AC), which is acceptable for use in businesses and homes. This process involves intricate adjustments and fine-tuning, which the control system manages in real-time to maintain efficiency and stability. Due to its critical role, the control system is a prime target for cyber-attacks. Malicious actors may attempt to infiltrate the control system to disrupt its operations, potentially causing significant damage or loss of functionality. For instance, by tampering with the control signals, hackers could alter the inverter's output, leading to inefficient energy conversion or even complete system failure.

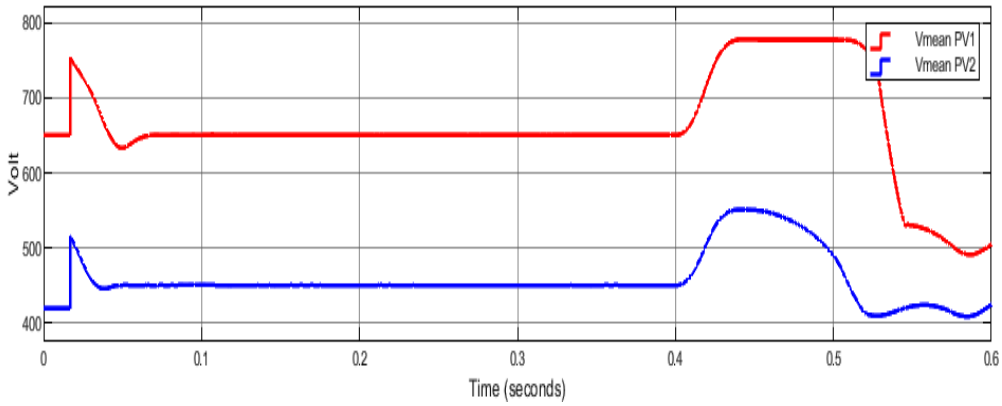
Such vulnerabilities underscore the necessity of robust cybersecurity measures to protect the control unit from unauthorized access and malicious activities. Figure.7 contains four internal shapes. The first one represents the irradiance. The second subfigure represents the duty cycle (D) of the MPPT value of the control system for each PV cell, where MPPT Maximum power point tracking changes the duty cycle automatically by controlling the switch to obtain the required voltage, and thus the maximum power can be extracted. The third subfigure represents the mean voltage of each PV. The fourth subfigure represents the mean (DC) current of each PV. It clears the response of the control center according to the changes that occur in the system. The attack happened at time 0.4, which is clear in all subfigures. That led to increased duty cycle as well as voltage. Also, it causes a decrease in current. Figure 8 represents the system's output for 3-phases.



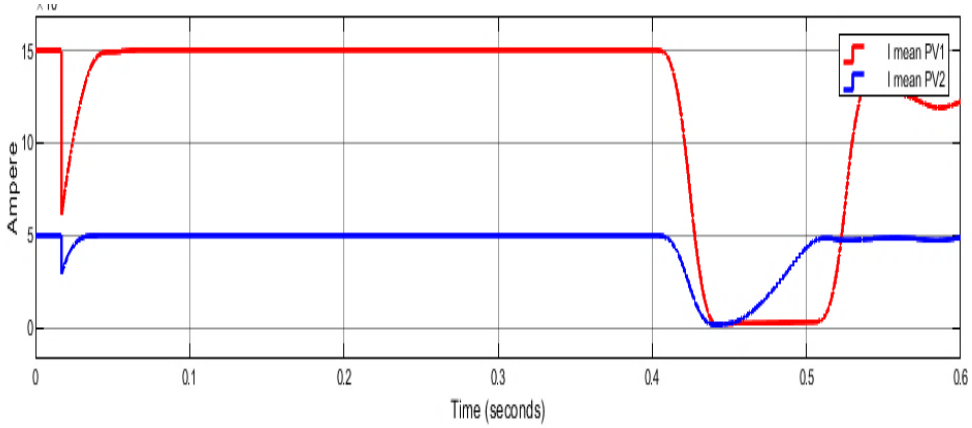
(a) Irradiance of PV



(b) Duty Cycle for MPPT



(c) DC-DC Voltage of PV



(d) DC-DC Current of PV

Figure 7. The response of the TDA of the control unit.

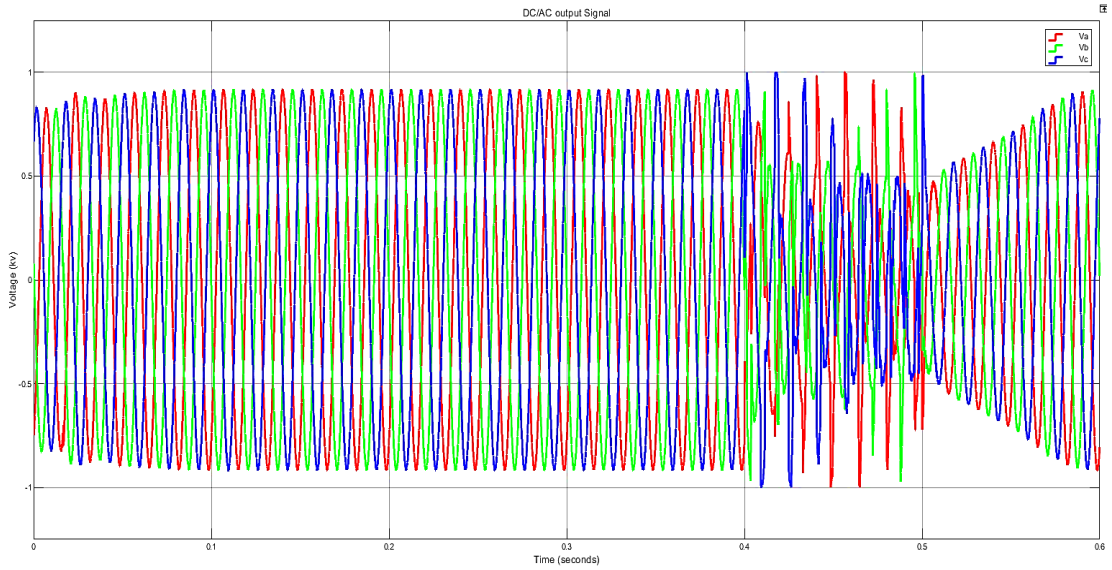


Figure 8. The system's output for the three phases.

As shown in Figure 8, a simulation of the DC/AC controller attack shows distortions that represent significant changes in the output waveform at time 0.4, which represents the attack time. Given that these changes pose a potential risk, the network behavior leads not only to large anomalies but also to subtle distortions in the DC inverter signal waveform shown in Figure 9, making attack detection and diagnosis difficult. As is clear, the impact of the

electronic time delay attack appears at a time of 0.4 to 0.5, which represents the time to simulate the attack.

Due to the electronic attack, the controller signals will be delayed and out of synchronization. For example, the duty cycle disturbance shown in Figure 7 during the attack period will cause the MPPT to fail to transmit maximum power, i.e. the station power = 0 at the DC converter, so the current will also = 0, i.e. the converter will act as an open circuit. This event will result in a significant increase and change in the voltage value as shown in Figure 9.

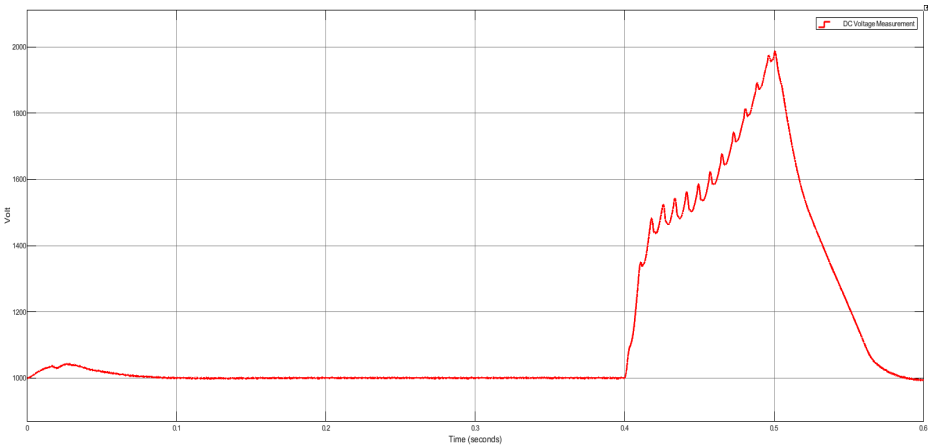
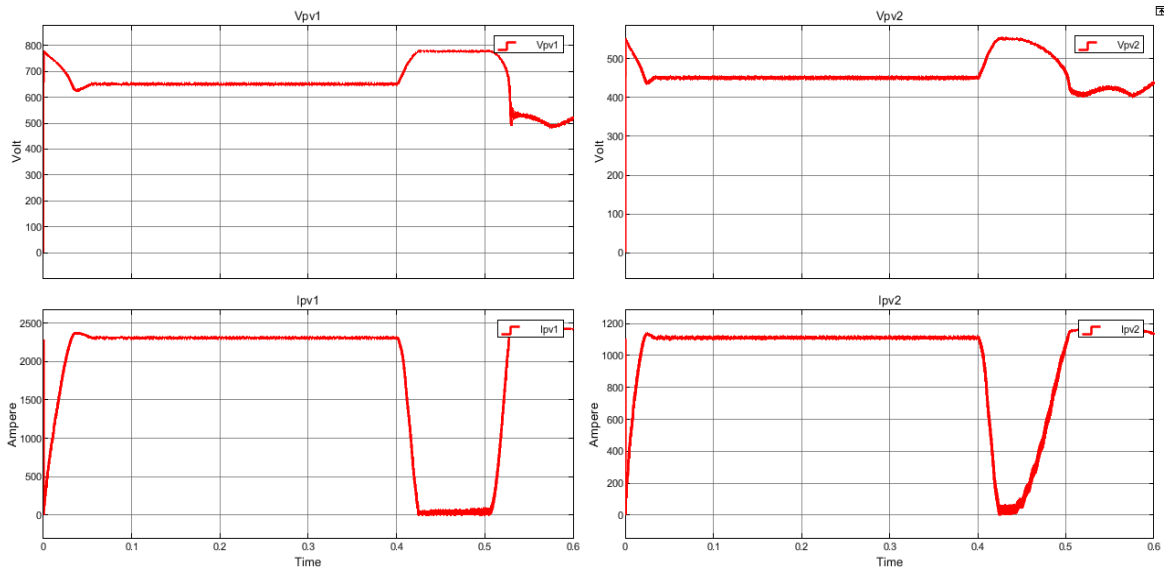


Figure 9. The output voltage of DC/DC.

Figure 10 represents the fixed output voltage from the solar cells as well as the current value of SCF waveforms of the solar inverter and their impact on the cells, assuming that the attacker can arbitrarily change the sensor measurements and illegally access grid-connected PV farm assets where the fault at 0.4 is simulated using the same TDA. It clears the fault of the voltage and current, which is harsher than the stream resulting from the cyber-attack described above. SCF distorts the voltage and current as well. It is difficult to see that this fault causes sudden and transient effects on high currents, voltages, and asymmetric components in the steady state and exposes the station control unit to danger. Their ultimate goal is to affect grid stability, cause tragic failure, and cause significant economic and physical damage.

.

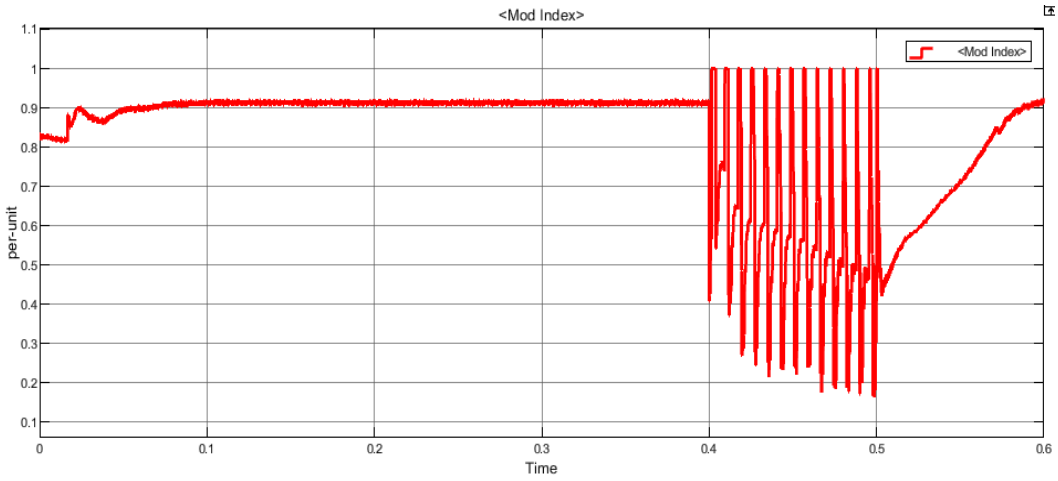


(a) Voltage and Current of PV1 (b) Voltage and Current of PV2

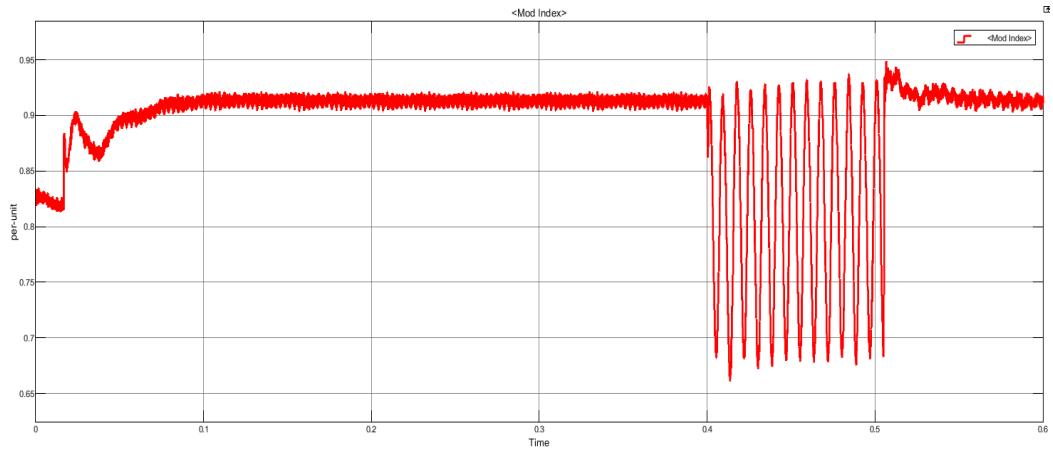
Figure 10. The output voltages from the solar cells as well as the currents of the SCF.

This type of error certainly leads to an increase in the value of the current to infinity at the attack node, which may be in the transformers or the feeders in the grid, which leads to a stop or delay in the operation of the DC/DC converter during the simulation period, thus leading to a decrease in the value of the direct electric current so that it becomes an open circuit. The presence of an attack that simulates the conditions referred to can lead to the result shown in Figure 10. As for the increase in the value of the voltage, it is equivalent to the presence of an open circuit at the output of the DC/DC converter.

Figure 11(a) represents the response of the Mod-index that clearly shows the moment of electronic attack at time 0.4. It is one of the important signals for the control signals of the inverter. This type of error certainly leads to a decrease in the value of the electric current to the end-user or the network, as the presence of an attack that simulates the conditions referred to can lead to the result shown in Figure 10. As for the increase in the voltage value, it is equivalent to the presence of an open circuit due to stopping or delaying the operation of the inverter system. We notice that the inverter returns to a stable state after the attack, but gradually, while Figure 11(b) shows the same signal, but in the case of a short-circuit fault. The attacker often performs this intentional fault on his ground, so that the signal of the Mod-index in the inverter returns directly to its state after the end of the short circuit and not gradually as in the time delay attack shown in Figure 11(a).



(a) Cyberattack TDA



(b) Physical attack SCF

Figure 11. Illustrate the waveforms of the Mod-index response

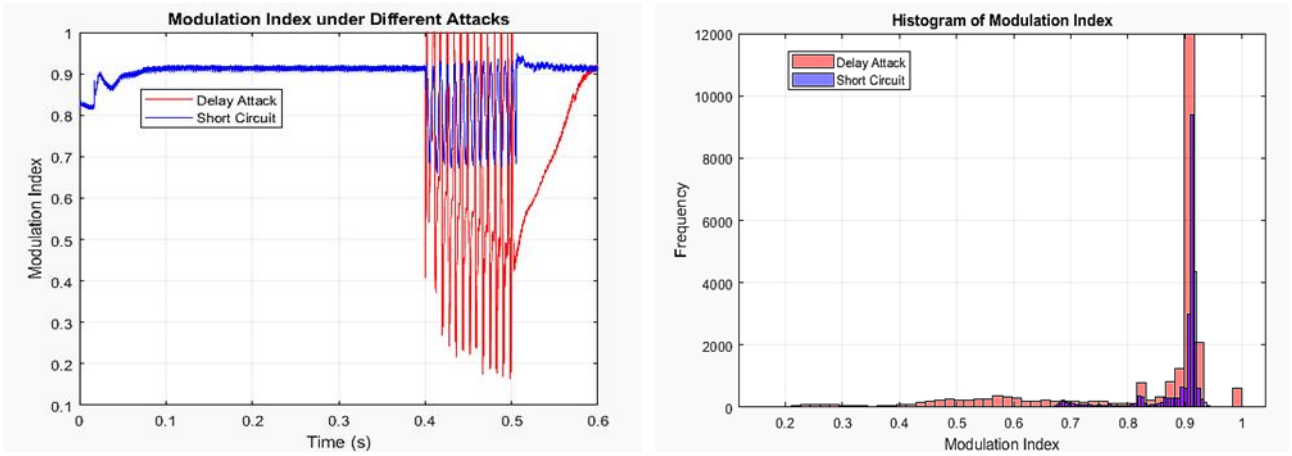
The time 0.4 is just the simulated attack time. Any other time could have produced almost similar results. THD is calculated for both attacks according to Table 1. As shown in Table 1, the THD of TDA is lower than that of SCF. This is due to the newness of the attack technology and the weakness of THD in diagnosing it. As a result, the importance of the Mod-index in diagnosing the attack is highlighted.

Table 1: Harmonic for both attack scenarios at 0.4s

	THD
Time Delay Attack	1.142
Short Circuit Fault	2.1673

6. Statistical analysis

To demonstrate the usefulness of the Mod-index in diagnosing attack types, it is necessary to combine the Mod-index of attacks and analyze them statistically. Fig. 12 shows the waveforms related to the Mod-index response.



(a) Mod-index histogram

(b) The Mod-index attacks are combined

Figure 12. Illustrate the waveforms of the Mod-index response

The histograms in Figure 12 (a) show that the distribution of the Mod-index values in the time delay case is closer to a skewed distribution, with long outliers in the lower ranges, reflecting increasing disturbance over time. The values in the SCF case were more concentrated around the mean, indicating relative stability after the attack.

Table 2: Statistical analysis of signals generated by Mod-index attacks

	Mean	StdDev	Max	Min
TDA	0.82163	0.1676	1	0.16402
SCF	0.89026	0.05455	0.9484	0.66062

The Mod-index behavior of a PV system subjected to two different attacks: time-delay and SCF, was analyzed to assess the impact of each attack type on system stability and productivity.

Based on Table 2, the mean of Mod-index for TDA is 0.8216 with a standard deviation of 0.1676, while the SCF recorded a higher mean of 0.8902, but with a much lower standard deviation of 0.054. These results reflect

a clear contrast in the system's behavior under each attack type. A high standard deviation for the TDA condition indicates that the signal is subject to large and irregular fluctuations over time, threatening the system's stability and long-term operation, potentially leading to controller failure or inverter and battery performance malfunctions.

In contrast, SCA causes a sharp and immediate drop in the Mod-index, but this occurs within a relatively narrow range (0.66–0.94) and is characterized by greater regularity after the attack. Although the change is sudden, the stability of the signal after the fault may allow the system to detect and respond more quickly, compared to gradual disturbances caused by time delay.

Accordingly, it can be argued that TDA is more dangerous in the long run due to its subtle and cumulative effects and the difficulty of detecting it at the outset. SCF, while it has a severe impact, is more likely to be detected early due to the abrupt nature of the change.

7. Conclusions

This paper presents a modeling and detection of cyber and physical attacks on the control unit of the PV farm system. Total harmonic distortion (THD) is employed in the proposed system to contribute to the detection of attacks. The THD metric proved crucial in detecting sudden changes in current and voltage waveforms, allowing the identification of anomalies caused by cyberattacks (TDA) and physical attacks (SCF). However, diagnosing the type of attack remains a difficult task, especially since both types of attacks occur at the same time of 0.4 second.

On the other hand, the Mod-Index played a crucial role in diagnosing the type of attack and its impact on the PV control unit, where in the best case of good operation of the PV at 0.9, it drops below 0.2 under the influence of TDA with a time delay that lasts to 0.6 seconds, while it drops to below 0.7 under the influence of SCA without a time delay. In this context, comparing the histograms of the two signals reveals that the distribution of values in the time delay case is more dispersed, while the distribution of values in the SCF case is more concentrated around the mean. This difference in statistical behavior can be used later to develop intelligent detection systems based solely on the behavior of the Mod-index to detect and diagnose the type of attack.

The proposed framework can be used as a smart indicator to help detect cyber-attacks or system errors, such as short circuits, but that is required to be integrated within smart monitoring and control systems. Also, the Mod-index can be linked to anomaly detection algorithms using artificial intelligence or machine learning.

For more security improvements, we propose future work to integrate advanced technologies, such as machine learning and AI-powered anomaly detection, while maintaining the efficiency of TDA or other attack techniques, mitigating inherent timing issues, and building a robust cybersecurity framework.

References

[1] F. A. Rahim, N. A. Ahmad, P. Magalingam, N. Jamil, Z. C. Cob, and L. Salahudin, "Cybersecurity vulnerabilities in smart grids with solar photovoltaic" a threat modelling and risk assessment approach. International Journal of Sustainable Construction Engineering and Technology, vol. 14, no. 3, pp. 210-220, 2023, DOI: https://doi.org/10.30880/ijscet.2023.14.03.018.

[2] U. Inayat, M. F. Zia, S. Mahmood, T. Berghout, and M. Benbouzid " Cybersecurity enhancement of smart grid: Attacks, methods, and prospects. Electronics", vol. 11, no. 23, pp. 3854, 2022, Doi: https://doi.org/10.3390/electronics11233854.

[3] S. Burande, A. Nawale, and D. Zade, "Modeling and Simulation of Solar System with MPPT Based Inverter and Grid Synchronization". International Research Journal of Engineering and Technology (IRJET), vol. 10, no. 5, pp. 2395-0072, 2023.

[4] B. O. Olorunfemi, N. I. Nwulu, and O. A. Ogbolumani, " Solar panel surface dirt detection and removal based on arduino color recognition". MethodsX, vol. 10, 101967, 2023, DOI: https://doi.org/10.1016/j.mex.2022.101967.

[5] N. Yılankırkan, and B. C. Baytar, " Development of Photovoltaic Systems and Application in Smart Grids: Sivas Case, " vol.13, no. 2, 2024, DOI: 10.18421/TEM132-78.

[6] Kareem, Parween R., et al. "Enhancing PV Power Extraction Under Partial Shading Condition with Shade Dispersion Strategy." Diyala Journal of

Engineering Sciences,Vol. (17), No. 1, pp. 38-50, 2024, DOI: 10.24237/djes.2024.17104.

[7] S. R. Pendem, and S. Mikkili, "Modeling, simulation and performance analysis of solar PV array configurations (Series, Series–Parallel and Honey-Comb) to extract maximum power under Partial Shading Conditions," Energy Reports, vol. 4, pp. 274-287, 2018, DOI: https://doi.org/10.1016/j.egyr.2018.03.003.

[8] S. N. Vodapally, and M. H. Ali, "Overview of intelligent inverters and associated cybersecurity issues for a grid-connected solar photovoltaic system, " Energies, vol. 16, no. 5904, pp. 1-19, 2023, https://doi.org/10.3390/en16165904.

[9] M. S. Ramkumar, R. F. Rajakumari, N. Kannan, R. Premkumar, S. Mohanasundaram, S. Purushotham, and K. Rajan, " Semiconductor Materials for Solar PV Technology and Challenges towards Electrical Engineering," Advances in Materials Science and Engineering, vol. 1, no. 7272489, pp. 1-6, 2022, https://doi.org/10.1155/2022/7272489.

[10] L. P. S. S. Panagoda, R. A. H. T. Sandeepa, W. A. V. T. Perera, D. M. I. Sandunika, S. M. G. T. Siriwardhana, M. K. S. D. Alwis, and S. H. S. Dilka, "Advancements in Photovoltaic (Pv) Technology for Solar Energy Generation," Journal of Research Technology & Engineering, vol. 4, no. 30, pp. 30-72, 2023.

[11] K. N. Nwaigwe, P. Mutabilwa, and E. Dintwa, "An overview of solar power (PV systems) integration into electricity grids". Materials Science for Energy Technologies, vol. 2, no. 3, pp. 629-633, 2019, https://doi.org/10.1016/j.mset.2019.07.002.

[12] O. M. Benaissa, S. Hadjeri, S. A. Zidi, and O. M. Benaissa, " Modeling and simulation of grid connected PV generation system using Matlab/Simulink," International Journal of Power Electronics and Drive System (IJPEDS), vol. 8, no. 1, pp. 392-401, 2017, DOI: 10.11591/ijpeds.v8i1.pp392-401.

[13] BAHAR, Saif Talal; RASHID, Yasir G. A Study on An MPPT Control Approach Using Artificial Intelligence and the Perturb and Observe Method. Diyala Journal of Engineering Sciences, Vol (17) No 2, pp.131-143, 2024, DOI: 10.24237/djes.2024.17210.

[14] M. Alharbi, "Control Approach of Grid-Connected PV Inverter under Unbalanced Grid Conditions. Processes", vol. 12, no. 1, pp. 212, 2024, https://doi.org/10.3390/pr12010212.

[15] Z. M. S. Elbarbary, and M. A. Alranini, " Review of maximum power point tracking algorithms of PV system," Frontiers in Engineering and Built Environment, vol. 1, no. 1, pp. 68-80, 2021, DOI: 10.1108/FEBE-03-2021-0019.

[16] S. Dash, and V. P. Kumri, " A Design of 400 KW Photovoltaic Array Connected Micro Grid System Using Matlab Simulink Model," Intern. J. Advanced Research in Electrical, Electronics and Instrumentation Eng, vol. 7, no. 12, pp. 4257-4262, 2018, DOI:10.15662/IJAREEIE.2018.0712019.

[17] A. El Hammoumi, S. Chtita, S. Motahhir, and A. El Ghzizal, " Solar PV energy: From material to use, and the most commonly used techniques to maximize the power output of PV systems," A focus on solar trackers and floating solar panels, Energy Reports, vol. 8, pp. 11992-12010, 2022, https://doi.org/10.1016/j.egyr.2022.09.054.

[18] P. T. Le, H. L. Tsai, and P. L. Le," Development and performance evaluation of photovoltaic (PV) evaluation and fault detection system using hardware-in-the-loop simulation for PV applications," Micromachines, vol. 14, no. 674, pp.1-19, 2023, https:// doi.org/10.3390/mi14030674.

[19] J. H. Lee, J. Shin, and J. T. Seo, " Solar Power Plant Network Packet-Based Anomaly Detection System for Cybersecurity". Computers, Materials & Continua, vol. 77, no. 1, pp. 758-779, 2023, DOI: 10.32604/cmc.2023.039461.

[20] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, and M. A. Abbaszada, "A review of cyber–physical security for photovoltaic systems," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 4, pp. 4879-4901, 2021, DOI: 10.1109/JESTPE.2021.3111728.

[21] Q. Li, F. Li, J. Zhang, J. Ye, W. Song, and A. Mantooth, " Data-driven cyberattack detection for photovoltaic (PV) systems through analyzing micro-PMU data," In 2020 IEEE Energy Conversion Congress and Exposition (ECCE), pp. 431-436, 2020, DOI: 10.1109/ECCE44975.2020.9236274.

[22] F. Li, Q. Li, J. Zhang, J. Kou, J. Ye, W. Song, and H. A. Mantooth, "Detection and diagnosis of data integrity attacks in solar farms based on multilayer long short-term memory network," IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 2495-2498, 2020, DOI: 10.1109/TPEL.2020.3017935.

[23] X. Gao, M. Ali, and W. Sun, "A Risk Assessment Framework for Cyber-Physical Security in Distribution Grids with Grid-Edge DERs," Energies, vol. 17, no. 1587, pp. 1-24, 2024, DOI: https://doi.org/10.3390/en17071587.

[24] J. Zhang, L. Guo, J. Ye, A. Giani, A. Elasser, W. Song, and H. A. Mantooth, " Machine learning-based cyber-attack detection in photovoltaic farms," IEEE Open Journal of Power Electronics, 2023, DOI: 10.1109/OJPEL.2023.3309897.

[25] T. Kaewnukultorn, S. B. Sepúlveda-Mora, R. Broadwater, D. Zhu, N. G. Tsoutsos, and S. Hegedus, " Smart PV Inverter Cyberattack Detection Using Hardware-in-the-Loop Test Facility," IEEE Access, vol. 4, pp.1-14, 2023, DOI: 10.1109/ACCESS.2023.3308052.

[26] L. Guo, J. Zhang, J. Ye, S. J. Coshatt, and W. Song, " Data-driven cyber-attack detection for pv farms via time-frequency domain features," IEEE Transactions on smart grid, vol. 13, no. 2, pp. 1582-1597, 2021, DOI: 10.1109/TSG.2021.3136559.

[27] H. H. Abed, A. S. Shaeel, and R. S. A. Annoze, " Hiding algorithm based fused images and Caesar cipher with intelligent security enhancement," International Journal of Electrical & Computer Engineering, vol. 13, no. 6, pp. 6797-6805, December 2023, DOI: 10.11591/ijece.v13i6.pp6797-6805.

[28] F. Harrou, B. Taghezouit, B. Bouyeddou, and Y. Sun, "Cybersecurity of photovoltaic systems: challenges, threats, and mitigation strategies: a short survey," Frontiers in Energy Research, vol. 11, no. 1274451, 2023, DOI 10.3389/fenrg.2023.1274451.

[29] B. Achaal, M. Adda, M. Berger, H. Ibrahim, and A. Awde, " Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges," Cybersecurity," vol. 7, no. 10, pp. 1-30, 2024, https://doi.org/10.1186/s42400-023-00200-w.

[30] F. Li, R. Xie, B. Yang, L. Guo, P. Ma, J. Shi, and W. Song, " Detection and identification of cyber and physical attacks on distribution power grids with pvs: An online high-dimensional data-driven approach," IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 10, no. 1, pp. 1282-1291, 2019, DOI: 10.1109/JESTPE.2019.2943449.

[31] Zhou, Y.; Ghosh, S.; Ali, M.H.; Wyatt, T.E. Minimization of Negative Effects of Time Delay in Smart Grid System. In Proceedings of the 2013 Proceedings of IEEE Southeastcon, Jacksonville, FL, USA, 4–7 April 2013, DOI: 10.1109/SECON.2013.6567474.

[32] Macana, C.A.; Mojica-Nava, E.; Quijano, N. Time-Delay Effect on Load Frequency Control for Microgrids. In Proceedings of the 2013 10th IEEE International Conference on Networking, Sensing and Control, Evry, France, 10–12 April 2013; pp. 544–549, DOI: 10.1109/ICNSC.2013.6548797.

[33] Musleh, A.S.; Muyeen, S.M.; Al-Durra, A.; Kamwa, I.; Masoum, M.A.S.; Islam, S. Time-Delay Analysis of Wide-Area Voltage Control Considering Smart Grid Contingences in a Real-Time Environment. IEEE Trans. Ind. Inf. , 14,p.p. 1242–1252,2018, DOI: 10.1109/TII.2018.2799594.

[34] R. Sinvula, K. M. Abo-Al-Ez, and M. T. Kahn, “Total harmonics distribution (THD) with PV system integration in smart grids: Case study,” 2019 International Conference on the Domestic Use of Energy (DUE), IEEE Xplore, pp. 102–108, 2019.

[35] H. P. Devarapalli, V. Dhanikonda, and S. B. Gunturi, “Non-intrusive identification of load patterns in smart homes using percentage total harmonic distortion,” Energies, vol. 13, no. 18, pp. 4628, 2020, https://doi.org/10.3390/en13184628.

[36] J. J. Q. Yu, Y. Hou, and V. O. K. Li, Online false data injection attack detection with wavelet transform and deep neural networks, IEEE Trans. Ind. Informat., vol. 14, no. 7, pp. 32713280, Jul. 2018. DOI: 10.1109/TII.2018.2825243.